Docket No. AUS920000814US1

CLAIMS:

What is claimed is:

1. A method in a data processing system for executing cryptographic operations, the method comprising:

responsive to a request to perform a cryptographic operation, selecting one of a software process and a hardware process for performing the cryptographic operation based on a policy which process results in a available resources to perform the cryptographic operation to form a selected process; and

performing the cryptographic operation using the selected process.

2. The method of claim 1, wherein the policy includes selecting the one based on available resources to perform the cryptographic operation.

3. The method of claim 1, wherein the policy includes selecting the one resulting in a fastest completion of the cryptographic operation.

4. The method of claim 1, wherein the selecting step includes:

selecting the one using a preference associated with the request.

5. The method of claim 4, wherein the preference is for the hardware process to performing the cryptographic operation.

6. The method of claim 1, wherein the cryptographic operation is an encryption of data using a key.

7. The method of claim 5, wherein the step of performing the cryptographic operation includes converting the key to a form useable by the selected process if the key is in a different form.

8. The method of claim 6, wherein the key is a hardware key and the selected process is the software process and further comprising:

converting the hardware key into a software form useable by the software process.

9. The method of claim 1, wherein the policy comprises a set of rules used to minimize available resources consumed in performing the cryptographic operation.

10. The method of claim 1, wherein the policy comprises a set of rules used to maximize a speed at which the cryptographic operation is performed.

11. A method in a data processing system for executing cryptography processes, the method comprising:

responsive to a request to perform a cryptographic operation, selecting from one of a software process and a hardware process for performing the cryptographic operation based on available resources to perform the cryptographic operation to form a selected process; and

performing the cryptographic operation using the

selected process.

12. The method of claim 11, wherein the cryptographic operation is one of a message digest and a public-private key encryption.

13. The method of claim 11, wherein the request is received from an application.

14. The method of claim 13, wherein the request is received from the application using an application program interface call made by the application.

15. The method of claim 11, wherein the cryptographic operation is an encryption of data using a key.

16. The method of claim 15, wherein the step of performing the cryptographic operation includes converting the key to a form useable by the selected process if the key is in a different form.

17. The method of claim 15, wherein the key is a hardware key and the selected process is the software process and further comprising:

converting the hardware key into a software form useable by the software process.

18. The method of claim 15, wherein the key is a software key and the selected process is the hardware process and further comprising:

converting the software key into a hardware form.

19. The method of claim 11, wherein the identified available resources include available processing resources and memory.

20. A data processing system comprising:

a bus system;

a communications unit connected to the bus, wherein data is sent and received using the communications unit;

a memory connected to the bus system, wherein a set of instructions are located in the memory; and

a processor unit connected to the bus system, wherein the processor unit executes the set of instructions to select one of a software process and a hardware process for performing the cryptographic operation based on a policy which process results in a available resources to perform the cryptographic operation to form a selected process in response to a request to perform a cryptographic operation; and perform the cryptographic operation using the selected process.

21. The data processing system of claim 20, wherein the bus system includes a primary bus and a secondary bus.

22. The data processing system of claim 20, wherein the processor unit includes a single processor.

23. The data processing system of claim 20, wherein the processor unit includes a plurality of processors.

24. The data processing system claim 20, wherein the

communications unit is an Ethernet adapter.

25. A data processing system comprising:

a bus system;

a communications unit connected to the bus, wherein data is sent and received using the communications unit;

a memory connected to the bus system, wherein a set of instructions are located in the memory; and

a processor unit connected to the bus system, wherein the processor unit executes the set of instructions to select from one of a software process and a hardware process for performing the cryptographic operation based on available resources to perform the cryptographic operation to form a selected process in response to a request to perform a cryptographic operation; and perform the cryptographic operation using the selected process.

26. A data processing system for executing cryptographic operations, the data processing system comprising:

selecting means for selecting one of a software process and a hardware process for performing a cryptographic operation based on a policy which process results in a available resources to perform the cryptographic operation to form a selected process in response to a request to perform the cryptographic operation; and

performing means for performing the cryptographic operation using the selected process.

27. The data processing system of claim 26, wherein the

policy includes selecting the one based on available resources to perform the cryptographic operation.

28. The data processing system of claim 26, wherein the policy includes selecting the one resulting in a fastest completion of the cryptographic operation.

29. The data processing system of claim 26, wherein the selecting means includes:

selecting means for selecting the one using a preference associated with the request.

30. The data processing system of claim 29, wherein the preference is for the hardware process to performing the cryptographic operation.

31. The data processing system of claim 26, wherein the cryptographic operation is an encryption of data using a key.

32. The data processing system of claim 30, wherein the performing means includes converting means for converting the key to a form useable by the selected process if the key is in a different form.

33. The data processing system of claim 31, wherein the key is a hardware key and the selected process is the software process and further comprising:

converting means for converting the hardware key into a software form useable by the software process.

34. The data processing system of claim 26, wherein the policy comprises a set of rules used to minimize available resources consumed in performing the cryptographic operation.

35. The data processing system of claim 26, wherein the policy comprises a set of rules used to maximize a speed at which the cryptographic operation is performed.

36. A data processing system for executing cryptography processes, the data processing system comprising:

selecting means for selecting from one of a software process and a hardware process for performing a cryptographic operation based on available resources to perform the cryptographic operation to form a selected process responsive to a request to perform the cryptographic operation; and

performing means for performing the cryptographic operation using the selected process.

37. The data processing system of claim 36, wherein the cryptographic operation is one of a message digest and a public-private key encryption.

38. The data processing system of claim 36, wherein the request is received from an application.

39. The data processing system of claim 38, wherein the request is received from the application using an application program interface call made by the application.

40. The data processing system of claim 36, wherein the cryptographic operation is an encryption of data using a key.

41. The data processing system of claim 40, wherein the performing means includes converting means for converting the key to a form useable by the selected process if the key is in a different form.

42. The data processing system of claim 40, wherein the key is a hardware key and the selected process is the software process and further comprising:

converting means for converting the hardware key into a software form useable by the software process.

43. The data processing system of claim 40, wherein the key is a software key and the selected process is the hardware process and further comprising:

converting means for converting the software key into a hardware form.

44. The data processing system of claim 36, wherein the identified available resources include available processing resources and memory.

45. A computer program product in a computer readable medium for executing cryptographic operations, the computer program product comprising:

first instructions, responsive to a request to perform a cryptographic operation, for selecting one of a

software process and a hardware process for performing the cryptographic operation based on a policy which process results in a available resources to perform the cryptographic operation to form a selected process; and

second instructions for performing the cryptographic operation using the selected process.

46. A computer program product in a computer readable medium for executing cryptography processes, the method comprising:

first instructions, responsive to a request to perform a cryptographic operation, for selecting from one of a software process and a hardware process for performing the cryptographic operation based on available resources to perform the cryptographic operation to form a selected process; and

second instructions for performing the cryptographic operation using the selected process.